Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 10 June 2005

Current Nationwide Threat Level is
ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS
For info click here
http://www.dhs.gov/

Daily Highlights

- China has discovered a strain of bird flu that is deadly to humans at a farm in the far western region of Xinjiang; more than 13,000 geese were slaughtered to curb its spread. (See item 14)
- The National Institute of Standards and Technology has released new risk assessment software that building owners and managers can use to identify and guard against terrorist threats to their facilities. (See item 26)

DHS/IAIP Update *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 09, Department of Energy* — **Secretary of Energy announces new energy office.** Secretary of Energy Samuel Bodman on Thursday, June 9, announced the completion of the merger of the former Office of Electric Transmission and Distribution and Office of Energy Assurance into the new Office of Electricity Delivery & Energy Reliability (OE). OE's goal is to lead national efforts to modernize the electric grid, enhance security and reliability of the energy infrastructure, and facilitate recovery from disruptions to energy supply. The merger was recommended by Congress and approved by Secretary Bodman in February 2005. Primarily, the office will support research, development, demonstration, technology transfer, and education and activities necessary to enhance national energy security. Partnerships to engage industry, utilities, States, other Federal programs and agencies, universities, national

laboratories, and other stakeholders in OE's efforts to ensure a more reliable, efficient, and affordable national electricity supply will continue to be a key element of the program. Kevin Kolevar, the Director of the Office of Electricity and Energy Assurance will head the office under its new name and structure.
Source: http://www.energy.gov/engine/content.do?PUBLIC_ID=18034&BT_CODE=PR_PRESSRELEASES&TT_CODE=PRESSRELEASE

2. *June 09, Long Island Power Authority* — **Electric utility tests how much electricity it can save.** The Long Island Power Authority (LIPA), the New York State Office of Emergency Management, KeySpan successfully conducted its second annual islandwide "I'm Ready" emergency preparedness drill Thursday, June 9. Businesses, municipalities and residential customers around Long Island voluntarily reduced electric use between the noon and 3 PM to demonstrate an active involvement in the emergency planning process. Local, county, and state emergency response entities also participated to exercise emergency response procedures and command and control centers. LIPA estimates that voluntary electric use reductions by its customers reduced electric use islandwide by about 90 to 100 megawatts (MW), which is enough to power about 90,000 to 100,000 averaged−sized Long Island homes. The annual "I'm Ready" drill, the largest of its kind in the nation, encourages LIPA customers to plan and prepare for a major emergency such as a Hurricane Gloria−like storm. Hurricane Gloria occurred 20 years ago and was the last full−strike hurricane to hit Long Island.
Source: http://www.lipower.org/newscenter/pr/2005/june9.drill.html

3. *June 08, MarketWatch* — **Power grid under mounting pressure.** As consumers turn up their air conditioners heading into the hottest months of the year, the network of power lines crisscrossing the United States faces heightened congestion amid greater demand, the nation's top energy regulator said Wednesday, June 8. Federal Energy Regulatory Commission Chairman Patrick Wood told a House panel that the 157,000 miles of high−power transmission lines in America is the weakest link in the power system, despite modest improvements made following a massive power outage in 2003 that left millions without power. Although industry has boosted investments in the grid in recent years, growth in transmission capacity is still lagging behind electricity demand, Wood said in testimony before the House Subcommittee on Energy and Resources. "We've seen an increase in congestion in almost every region of the country" at a cost of billions of dollars to consumers, Wood added. Industry officials acknowledge that demand has outpaced available capacity and investment. "Each year in the last decade, more transmission lines have been experiencing congestion for more hours of the year," said Michael Gent, head of the North American Electric Reliability Council, in testimony before the panel.
Testimony: http://www.ferc.gov/eventcalendar/Files/20050608124932−testi mony−wood.pdf
Source: http://www.marketwatch.com/news/story.asp?guid=%7B5F4E96AE−BDE9−4758−A8B0−EDBECB21C136%7D&siteid=google

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *June 09, WTOV (OH)* — **Propane gas leak causes evacuations in Ohio county.** A gas leak in Guernsey County, OH caused several businesses to evacuate Wednesday, June 8, for fear an

explosion could occur. Around 3:00 a.m. Wednesday morning, Cambridge fire crews were called to a propane gas leak at Valley Welding on State Route 209 in Cambridge, OH. Fire officials say a truck driver was refilling the 30,000−gallon propane tank, when the valve malfunctioned, and liquid propane started shooting out. Fire officials say they're biggest concern was the leak would catch fire. "Any spark, from a thermostat, from a telephone ringer, from a light switch, somebody flipping a cigarette, anything could make it explode," said Cambridge Fire Chief Bill Minter. A mile−long stretch along State Route 209 was evacuated. Experts from Valley Welding made it to the scene, and crews stopped the leak around 11:30 a.m.
Source: http://www.wtov9.com/news/4586318/detail.html

5. *June 09, Associated Press* — **One person killed in Illinois plant explosion.** Federal, state and private investigators toured a central Illinois manufacturing plant Thursday, June 9, to determine how soon production could resume after an explosion and fire that left one person dead and another injured. The Conair Corp. hair−care products plant in Rantoul, IL canceled three shifts each Thursday and Friday. The explosion occurred shortly before 9 p.m. Wednesday, June 8, in a room where denatured alcohol is mixed with other raw materials to make hair care products, company spokeswoman Stephanie Burris said. Firefighters reported at least six explosions after they arrived at the plant, which is in an industrial park just west of this city of 13,000 people about 15 miles north of Champaign. “The fire marshal said we had one of the best sprinkler systems he had ever seen and the room responded exactly the way it was built to do,” Burris said. The room where the explosion happened was designed to direct an explosion upward rather than outward, she said.
Source: http://cbs2chicago.com/illinois/IL−−RantoulExplosion−in/reso urces_news_html

6. *June 09, Washington Post* — **Over 100 evacuated in carbon monoxide scare.** More than 100 people, many of them in wheelchairs who attend a cerebral palsy program, were evacuated Thursday morning, June 8, from a building in northeast Washington, D.C. after being overcome by carbon monoxide fumes. Two people were taken to George Washington University Hospital for minor exposure. Fire and EMS officials said that a contractor used a gasoline−powered engine that caused a build−up of carbon monoxide inside the International Business Mall Building. Fire crews confirmed high readings of carbon monoxide in the building, which was closed to the public to allow it to air out.
Source: http://www.washingtonpost.com/wp−dyn/content//article/2005/0 6/09/AR2005060901175.html

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

7.

June 09, New York Times — **A scramble to protect personal information.** With the loss of an entire box of magnetic tape in the care of the United Parcel Service, containing personal information on nearly four million American customers of Citigroup, attention is again focused on protecting sensitive information. When so much commerce is conducted online and when just a few bits of stolen data −− a Social Security number, a name, an address, a date of birth −− can be turned into cash by opening false credit accounts, thieves have proved themselves skilled at getting the information they need. Combating the crooks requires a holistic approach to data security, said Mike Gibbons, a security consultant for the global technology services company Unisys, and the former chief of cybercrime investigations for the FBI. That includes creating more secure online access methods, robust customer authentication, hiring dedicated data security staff, and improving the way large amounts of consumer data are stored or moved. "All of these things have cost impacts," Gibbons said. "Businesses have to pony up the capital to change the way they are storing and holding data," said Gibbons.
Source: http://www.nytimes.com/2005/06/09/business/09data.html?

[Return to top]

Transportation and Border Security Sector

8. *June 10, WBBM−TV (IL)* — **Tanker truck explosion temporarily closes Kennedy Expressway.** A tanker truck carrying ether rolled over and exploded on the outbound Kennedy Expressway outside of Chicago Thursday morning, June 9, causing a large fire and the temporary closing of outbound lanes. A tanker truck carrying 6,000 gallons of ether overturned and burst into flames. It took firefighters and crews that specialize in hazardous material spills only a little over an hour to secure the scene. According to Fire Lt. Bill Toman, the tanker truck lost control and the cab separated from the trailer. “The trailer initially hit the wall, caught on fire. We were able to put that out real quickly,” Toman continued. The driver of the truck was not seriously hurt and told officials that an unknown vehicle cut him off, which caused him to swerve and roll over, said Illinois State Police Officer Tom Koch.
Source: http://cbs2chicago.com/topstories/local_story_160072718.html

9. *June 09, Government Accountability Office* — **GAO−05−761T: Amtrak: Management and Accountability Issues Contribute to Unprofitability of Food and Beverage Service (Testimony).** Amtrak has provided food and beverage service on its trains since it began operations in 1971. Amtrak has struggled since its inception to earn sufficient revenues and depends heavily on federal subsidies to remain solvent. While a small part of Amtrak’s overall expenditures, Amtrak’s food and beverage service illustrates concerns in Amtrak’s overall cost containment, management and accountability issues. Amtrak’s financial records show that for every dollar Amtrak earns in food and beverage revenue, it spends about $2—a pattern that has held consistent for all three years the Government Accountability Office (GAO) reviewed. In GAO’s estimation, Amtrak has lost a total of almost $245 million from fiscal year 2002 through fiscal year 2004 on food and beverage service. GAO found five different management controls that Amtrak did not fully exercise regarding oversight of its food and beverage service. Since GAO did not have sufficient time to obtain Amtrak’s comments, as required by government auditing standards, prior to this hearing, GAO anticipates making recommendations to Amtrak to improve its food and beverage service at a later time.
Highlights: http://www.gao.gov/highlights/d05761thigh.pdf

Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−761T

[Return to top]

Postal and Shipping Sector

10. *June 09, News−Leader (MO)* — **Postal equipment will detect anthrax.** The U.S. Postal Service is a month away from being able to detect anthrax in letters processed at its Springfield, MO, facility. Anthrax spores that spread the disease are most effective when they're airborne, which can occur as letters are squeezed to be postmarked. "(A terrorist would want) that stuff dispersed somehow," said Tom Rebottaro, an inspector with the U.S. Postal Inspection Service. "And the best way of dispersing it is to send it through that cancelling equipment." Any detection would trigger a chain of events that would start with the complete evacuation of the facility. Public health officials would be notified to dispense medications to Postal Service employees and customers. And police would secure the scene until the FBI arrived. Postal inspectors would don biohazard suits to retrieve the air samples collected by the detector. The sample would be flown or driven to a lab for confirmation, which could take up to 48 hours.
Source: http://springfield.news−leader.com/news/today/20050609−Posta lequipment.html

[Return to top]

Agriculture Sector

11. *June 09, Yuma Sun (AZ)* — **Horse sites under quarantine.** A viral infection outbreak has put 28 horse properties around Arizona under quarantine. The virus is an untreatable but nonlethal ailment that can cause painful lesions in the mouth area and can spread readily to other horses as well as cattle and sheep. Since late April, 30 horses have been confirmed with the virus, state officials said. Most of the Arizona cases appear to involve leisure horses as opposed to commercial riding operations. The virus, called vesicular stomatitis, has put a bigger burden on horse owners and the organizers of equine events to ensure only healthy horses are traveling about the state.
Source: http://sun.yumasun.com/artman/publish/articles/story_17141.p hp

12. *June 09, Farm & Ranch Guide* — **Wheat leaf rust and stripe rust found in North Dakota.** Wheat leaf rust has recently been detected in spring and winter wheat in five counties in North Dakota. The detections occurred in Burleigh, LaMoure, Dickey, Cass, and Eddy counties. Severity levels of these rusts are very low at this time, but the widespread detection indicates that farmers need to be vigilant about these diseases and do frequent scouting, especially on susceptible cultivars, according to Marcia McMullen, North Dakota State University Extension plant pathologist. Leaf diseases can cause significant damage to wheat. Often that damage exceeds even the more obvious losses caused by weed competition. In North Dakota, small−grain yield losses due to leaf diseases have measured as high as 30 percent.
Source: http://www.farmandranchguide.com/articles/2005/06/09/ag_news /production_news/prod09.txt

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

13. *June 08, Maui News (HI)* — **Hawaii Department of Water Supply urges conservation.** A few heavy showers in May failed to reverse the trend toward a dry summer in most areas of Maui County, and the Department of Water Supply on Tuesday, June 7, issued an appeal for consumers to cut down on their use of water. The water department notice urged all Maui County residents to voluntarily reduce the amount of water they use, but cited Upcountry, West Maui, South Maui, Central Maui and Molokai as areas of specific concern. The National Weather Service is forecasting below−normal rainfall for most of the state, but specifies the islands of Maui County along with Oahu and the Big Island. According to the National Oceanic and Atmospheric Administration's Drought Outlook report, Molokai, Lanai, South Maui and West Maui already are considered to be "abnormally dry" while West Hawaii is rated as in "moderate drought." A key factor was the drier−than−normal spring. The monthly rainfall summaries reported by the National Weather Service indicate that most areas of Maui County recorded below−normal rainfall in April and May.
Department of Water Supply Website: http://www.hawaiidws.org/
Source: http://www.mauinews.com/story.aspx?id=9528

[Return to top]

Public Health Sector

14. *June 09, Reuters* — **China battles new outbreak of bird flu.** China has discovered a strain of bird flu that is deadly to humans at a farm in the far western region of Xinjiang. More than 13,000 geese were slaughtered to curb its spread, the Agriculture Ministry said on Thursday, June 9, after hundreds of dead geese were found on the farm in Xinjiang's Tacheng district and some 1,000 showed signs of illness. "The Xinjiang Veterinary Office, in accordance with animal epidemic prevention regulations, has adopted measures to seal off and sterilize the area," the ministry said in a statement. "Presently, the outbreak has been brought under control." Tests showed the cases were caused by the H5N1 virus, which first surfaced in poultry in Hong Kong and China eight years ago and has killed more than 50 people in Southeast Asia since it swept across large parts of the region in 2003.
Source: http://www.alertnet.org/thenews/newsdesk/SP218118.htm

15. *June 09, Agence France Presse* — **World health officials pin anti−malaria hopes on plant−based therapy.** World health advocates are increasingly looking to Artemisia annua, a plant traditionally used to fight fever, as a key weapon in the fight against malaria, experts said this week. Up to a million lives could be saved each year through wider use of so−called artemisinin−based combination therapies (ACTs), which are thought to be the most effective antimalarial medicines now available, they said. The benefits of extracts from the plant, also

known as "wormwood" and "sweet Annie," and ways to increase its production were the focus of a World Health Organization (WHO) conference here that wrapped up Wednesday, June 8. Extracts from the plant provide the basic chemical ingredients for ACTs and WHO officials want to ensure a reliable supply of artemisia.
Source: http://news.yahoo.com/s/afp/20050609/hl_afp/healthmalariawho_050609054143;_ylt=AiwX7Q7RkWfMG89ME2JKON.JOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

16. *June 09, Department of Homeland Security* — **DHS and American Red Cross co−sponsor National Preparedness Month 2005.** The Department of Homeland Security (DHS) and the American Red Cross today announced they will co−sponsor National Preparedness Month 2005, a nationwide effort held this September to encourage Americans to prepare for emergencies in their homes, businesses and schools. The goal of National Preparedness Month is to increase public awareness about the importance of preparing for emergencies and to encourage individuals to take action. DHS promotes public emergency preparedness through the Ready campaign and Citizen Corps. Ready is a national public service advertising campaign produced by the Advertising Council in partnership with DHS that is designed to educate and empower Americans to prepare for and respond to potential terrorist attacks and other emergencies. Citizen Corps, DHS's grassroots program, localizes Ready's preparedness messages and provides local opportunities for citizens to get emergency response training; participate in community exercises; and volunteer to support local emergency responders. Governed by volunteers and supported by community donations, the American Red Cross is a nationwide network of nearly 900 locally supported chapters dedicated to saving lives and helping people prevent, prepare for and respond to emergencies. For more information or to become a National Preparedness Month Coalition Member visit www.Ready.gov.
Source: http://www.dhs.gov/dhspublic/display?content=4538

17. *June 09, Paris Beacon News (IL)* — **Mistake in Illinois emergency drill draws concern.** A mistake in procedure during the emergency drill Tuesday, June 7, at the Edgar County Airport in Illinois caused concern from everyone involved. Assistant county emergency coordinator Duane Fidler confirmed that a teen volunteer was accidentally injected with an authentic antidote for nerve agent contamination during the mock emergency. "The teen was always under observation and exhibited no ill effects and no change in vital signs," Fidler said. Officials are looking at which antidote was used by the medical personnel on the scene who were suited and giving triage. Coordinator Terry Hackett said the auto injectors used in the drill are simulations of the actual anti−agent injectors that when pressed against the leg deliver a spring−loaded injection. The practice injectors are clearly marked and also give a "click and

go" sound. Another drill−related mishap occurred Wednesday when high temperatures overcame volunteers wearing butyl rubber protective gear at the Newport Chemical Plant in Indiana. One of the workers was transported via ambulance to West Central Community Hospital. The field portion of the exercise was suspended at approximately 1 p.m. and all workers were directed to remove protective apparel, cool off and rehydrate.
Source: http://www.parisbeacon.com/index.php?option=content&task=view&id=1305&Itemid=

18. *June 08, Department of Homeland Security* — **Department of Homeland Security launches Listo Negocios.** The Department of Homeland Security (DHS), in partnership with the Advertising Council, on Wednesday, June 8, launched Listo Negocios. This extension of the Listo campaign, which educates and empowers Spanish−speaking individuals to prepare for and respond to potential terrorist attacks and other emergencies, focuses on business preparedness. Listo Negocios will help Spanish−speaking owners and managers of small to medium−sized businesses prepare their employees, operations and assets in the event of an emergency. One of the key findings of the 9−11 Commission report was the need for the private sector to prepare for potential disasters. An emergency preparedness plan can greatly improve the likelihood that a company will survive and recover from all emergencies, natural disasters or terrorist attacks, but, too few businesses are taking the necessary steps to prepare. Listo Negocios is the Spanish version of the Ready Business campaign, which Homeland Security unveiled in September 2004. The Listo Negocios website (www.listo.gov) is designed to make emergency planning easier by providing businesses with practical steps and easy to use templates in Spanish to help them: plan to stay in business; talk to their employees; and protect their investment.
Source: http://www.dhs.gov/dhspublic/display?content=4534

19. *June 07, The Daily Sentinel (CO)* — **Mock disaster tests airports rescue units.** Grand Junction, CO, tested its preparedness Monday, June 6, during a full scale emergency exercise at Walker Field Airport. The mock−emergency involved a plane crashing into the Fed−Ex building, prompting a response from the airports' Aircraft Rescue Fire Fighting unit, the Grand Junction Fire Department, Grand Junction Police Department, Red Cross, Civil Air Patrol, Transportation Security Administration and Federal Bureau of Investigation. Responders acted as if it were a real crisis, treating false wounds and transporting patients to the hospital, with the exception of the ten fatalities− the dummies laid in a discarded heap by the end of the exercise. Overall the event went well, but there were some communications concerns, Fire Department Battalion Chief John Williams said. "Everyone has a lot to say and the radio channels get jammed up," which is not unusual during a large emergency, Williams said. A report that critiques the county's response will be released next week.
Source: http://www.gjsentinel.com/hp/content/news/stories/2005/06/07/6_7_emergency_drill.html;COXnetJSessionIDbuild78=CowukNFZ1Sayh2XfB8P2d0JWs65mAxa2Rgj6j1aNEW9n1ezQVvTe!−473512093?urac=n&urvf=11183678542180.5238012169347226

[Return to top]

Information Technology and Telecommunications Sector

20. *June 09, FrSIRT* — **Apple security update fixes multiple Mac OS X vulnerabilities.** Apple has released a security patch to correct multiple vulnerabilities affecting Mac OS X. These flaws could be exploited by remote or local attackers to execute arbitrary commands, cause a denial of service, obtain elevated privileges, or disclose sensitive information. Vendor updates are available. Mac OS X 10.3.9 Update (2005−006): http://www.apple.com/support/downloads/securityupdate2005006 macosx1039.html and Mac OS X 10.4.1 Update (2005−006): http://www.apple.com/support/downloads/securityupdate2005006 macosx1041.html
Source: http://www.frsirt.com/english/advisories/2005/0712

21. *June 09, SecurityFocus* — **Cisco Voice VLAN 802.1x authentication bypass vulnerability.** Cisco switches are susceptible to an authentication bypass vulnerability, allowing attackers to gain anonymous access to the voice VLAN. Attackers may spoof CDP packets, and impersonate a Cisco IP phone, in order to anonymously join the voice VLAN. This allows attackers to gain access to network resources without the expected 802.1x authentication sequence. As network administrators expect that switch port access is restricted to only authenticated users, a false sense of security may pervade. Vendor advisory and workarounds: http://www.cisco.com/warp/public/707/cisco−sn−20050608−8021x .shtml
Source: http://www.securityfocus.com/bid/13902/discuss

22. *June 09, NewScientist* — **New type of virus scans networks for vulnerabilities.** An emerging breed of computer virus that keeps hackers informed about the latest weaknesses in computer networks has been discovered by security experts. The viruses infect a computer network, scan for security vulnerabilities and then report back to hackers through an Internet chatroom. Armies of computers infected with "bot" viruses are routinely controlled via a chatroom connection and are used to knock for denial of service attacks or as a conduit for sending out spam e−mail. However, the ability of some bots to scan their hosts for unpatched security holes and report their findings back to hackers has gone largely unnoticed until now. The emerging class of malware or malicious software − known as vulnerability assessment worms − "phone home" to allow hackers to fine−tune further attacks or perhaps even target an individual PC within a network. This pernicious form of program is just one of a growing number of new viruses identified each month, says computer security expert Bruce Schneier. "The virus trend doesn't look good," Schneier writes in the June 2005 edition of the Association for Computing Machinery journal, Queue. "More than a thousand new worms and viruses were discovered in the last six months alone."
Source: http://www.newscientist.com/article.ns?id=dn7500

23. *June 09, New York Times* — **Internal audit finds DHS is lacking disaster backups.** An internal inspector general audit released on Wednesday, June 8, concluded the computer systems at 19 Department of Homeland Security (DHS) sites that served agencies like the Transportation Security Administration, Customs and Border Protection and the Coast Guard had no functioning backups or relied on obviously deficient or incomplete backups. Even the Federal Emergency Management Agency, which is in charge of disaster recovery, was unprepared, the report said. The department "must be able to provide mission−essential services with minimal disruption following a disaster," the report said. Adequate backups were lacking for networks that screen airline passengers, that inspect goods moving across borders and that communicate with department employees and outside officials. Those same agencies, the

auditors found, have in most cases failed to prepare sufficiently written disaster recovery plans that would guide operations if a main office or computer system was knocked out. The problems, the audit said, are insufficient money and insufficient management attention. "We recognize that information−technology continuity is important to lead an effective recovery, which is why we are developing a plan to ensure critical systems continuity," a spokesperson, Brian Roehrkasse, said.
Inspector General's Report: http://www.dhs.gov/interweb/assetlibrary/OIGr_05−22_May05.pd f
Source: http://www.nytimes.com/2005/06/09/politics/09home.html

24. *June 08, SecurityTracker* — **IBM AIX buffer overflows let local users execute arbitrary code.** Several vulnerabilities were reported in IBM's AIX operating system, affecting the vscout, paginit, diagTasksWebSM, getlvname, and swcons commands and multiple "p" commands. A local user can supply specially crafted command line parameters to trigger a buffer overflow in the invscout, paginit, diagTasksWebSM, getlvname, and swcons commands and execute arbitrary code, potentially with root privileges. No solution is currently available.
Source: http://www.securitytracker.com/alerts/2005/Jun/1014132.html

25. *June 08, Federal Computer Week* — **Cybersecurity plagues Fort Hood army base.** Fort Hood, TX, the largest Army base in the world and home of the 4th Infantry Division −− the service's first digitized force −− has a huge information security problem, said Major General Dennis Moran, the Army's director of information operations, network and space in the Office of the Chief Information Officer. He spoke June 8 at the Army Information Technology Conference sponsored by the Army Small Computer Program. Some Army IT leaders think the best way to solve the information security problem at Fort Hood is to operate IT as an enterprise. For example, the base has 96 domains on the military's unclassified network. Consolidating e−mail, servers and storage systems would improve network management, operations and security, Moran said. But Fort Hood technology workers resisted the consolidation idea. The Army's IT leaders must resolve the tension between the Army's need to operate IT as an enterprise and IT workers' unique requirements at bases, Moran said.
Source: http://www.fcw.com/article89132−06−08−05−Web

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: The US−CERT has received reports from the private sector of potential widespread infections of new variants of the Mytob worm via social engineering techniques. The new variants are using emails that appear to be from internal IT staff reporting problems with the user's account and directing them to a URL where the malcode can be downloaded. The variants are described as mass mailing worms that have back door capabilities and use their own SMTP engine to send an email to addresses gathered from the compromised

computer. Although both variants have been categorized with an overall low severity rating and present no new threat, the fact that some organizations have experienced and reported a surge of infections at least warrants a renewed caution.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 6881 (bittorrent), 27015 (halflife), 1026 (−−−), 139 (netbios−ssn), 53 (domain), 32775 (sometimes−rpc13), 1434 (ms−sql−m), 80 (www) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

26. *June 09, Continuity Central* — **New risk assessment software addresses building threats.** National Institute of Standards and Technology (NIST) economists have released new risk assessment software that building owners and managers can use to identify and guard against terrorist threats to their facilities. The software, developed by NIST's Office of Applied Economics (OAE) as part of NIST's commitment to homeland security, is the finished version of a beta program released last year for limited testing. The Cost Effectiveness Tool for Capital Asset Protection (CET), Version 1.0, employs a three−step process for developing a risk mitigation plan. Its essential components are risk assessment; identification of potential mitigation strategies; and economic evaluation. CET first allows users to look at possible damage scenarios. Users then can explore strategies to reduce facility vulnerability. Choices include engineering alternatives (such as sensors to detect airborne contaminants); management practices (such as evacuation drills or increased security) and financial mechanisms (such as tax−write offs for capital improvements). Finally, CET users can evaluate the actual life−cycle costs (planning, installation and maintenance) of the various mitigation strategies. The combination of strategies that reflects the lowest life−cycle cost is designated the cost−effective risk mitigation plan.
Software: http://www2.bfrl.nist.gov/software/CET/
Source: http://continuitycentral.com/news01919.htm

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer